

3

Sheet 1 of 1

Form PTO-1449 (modified)	Attorney Docket No. ARC920010005US1	Serial No. Unk.
LIST OF PATENTS AND PUBLICATIONS FOR APPLICANT(S)' INFORMATION DISCLOSURE STATEMENT (Use several sheets if necessary)	Applicant(s): LOTSPIECH et al.	
	Filing Date: Herewith	Group Art Unit: Unk.

1098238.8 PTO
08/17/00
01/26/01

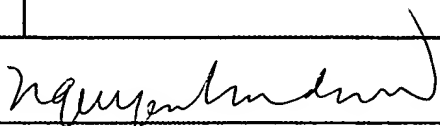
U.S. PATENT DOCUMENTS

Examiner Initials	Document No.	Date	Name	Class	Subclass	Filing Date
mon	6,138,119	10/24/00	Hall et al.	707	9	
↓	6,098,056	08/01/00	Rusnak et al.	705	75	

PUBLICATIONS / OTHER ART

Examiner Initials	Citation
mon	PUBLICATION: "Secure Group Communications Using Key Graphs". Wong et al. Proceedings of ACM SIGCOMM. Pgs 1-12. September, 1998. Canada.
	PUBLICATION: "Efficient Communication-Storage Tradeoffs for Multicast Encryption". Canetti et al. EUROCRYPT 1999. Pgs. 459-474.
	PUBLICATION: "Key Establishment in Large Dynamic Groups Using One-Way Function Trees". McGrew et al. Submitted to IEEE Transactions on Software Engineering. Pgs. 1-13. May, 1999.
	PUBLICATION: "Multicast Security: A Taxonomy and Some Efficient Constructions". Canetti et al. Proc. of INFOCOM. Vol. 2, pp. 708-716. New York, March 1999.
↓	PUBLICATION: "Broadcast Encryption". CRYPTO 1992, LNCS Vol. 839, pp. 257-270, New York, March 1994.

Examiner



Date Considered

5/9/05

Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).



Sheet 1 of 1

Form PT0-1449 (modified)

Attorney Docket No.
ARC920010005US1Serial No.
09/770,877LIST OF PATENTS AND PUBLICATIONS FOR
APPLICANT(S)' INFORMATION DISCLOSURE STATEMENT

(Use several sheets if necessary)

Applicant(s): LOTSPIECH et al.

Filing Date:
01/26/01Group Art Unit:
2132

U.S. PATENT DOCUMENTS

Examiner Initials	Document No.	Date	Name	Class	Subclass	Filing Date
						SEP 17 2002

FOREIGN PATENT DOCUMENTS

Technology Center 2100

Examiner Initials	Document No.	Date	Country	Class	Subclass	Translation Yes No
mon	0 641 103 A	03/01/95	Europe	H04L9/08		Yes

PUBLICATIONS / OTHER ART

Examiner Initials	Citation
mon	Abdalla M. et al. "Key Management for Restricted Multicast Using Broadcast Encryption," IEEE/ACM Transactions on Networking, IEEE Inc. New York, U.S. Vol. 8 pp. 443-454. August 2000.
↓	Blundo C. et al. "Trade-Offs Between Communication and Storage in Unconditionally Secure Schemes for Broadcast Encryption and Interactive Key Distribution." Advances in Cryptology, Crypto '96. Proceedings of the 16th annual International Cryptology Conf. pp. 387-400. Santa Barbara, U.S. August 1996.
↓	Chor B. et al. "Tracing Traitors". Advances in Cryptology. Proceedings of the 14th annual International Cryptology Conf. pp. 257-270. Santa Barbara, U.S. August 1994.

Examiner

nquyenburdum

Date Considered

5/9/05

Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).



Sheet 1 of 2

Form PTO-1449 (modified)

Attorney Docket No.
ARC920010005US1Serial No.
09/770,877LIST OF PATENTS AND PUBLICATIONS FOR
APPLICANT(S) INFORMATION DISCLOSURE STATEMENT

(Use several sheets if necessary)

Applicant(s): LOTSPIECH et al.

Filing Date:
01/26/2001Group Art Unit:
2137

U.S. PATENT DOCUMENTS

Examiner Initials	Document No.	Date	Name	Class	Subclass	Filing Date
mon	5812670	09/22/1998	Micali	380	25	
↓	5675649	10/07/1997	Brennan et al.	380	21	
↓	5241597	08/31/1993	Bright	380	21	

PUBLICATIONS / OTHER ART

Examiner Initials	Citation
mon	PUBLICATION: "Sequential Traitor Tracing". R. Safavi-Naini and Y. Wang. CRYPTO 2000, LNCS vol. 1880, PP. 316-332, 2000.
	PUBLICATION: "Efficient Trace and Revoke Schemes". M. Naor and B. Pinkas. Financial Cryptography '2000, LNCS 1962, pp. 1-20, 2001.
	PUBLICATION: "Efficient Methods for Integrating Traceability and Broadcast Encryption". E. Gafni, Jessica Staddon and Yiqun Lisa Yin. CRYPTO '99, Springer-Verlag LNCS 1666, pp. 372-387, 1999.
	PUBLICATION: "Trials of Traced Traitors". Birgit Pfitzmann. Workshop on Information Hiding, Cambridge, UK, LNCS, Vol. 1174, Springer-Verlag, pp. 1-16, 1996.
	PUBLICATION: "Digital Signets: Self-Enforcing Protection of Digital Information". C. Dwork, J. Lotspiech and M. Naor. 28 th Symposium on the Theory of Computation, pp. 489-498, 1996.
	PUBLICATION: "An Efficient Public Key Traitor Tracing Scheme". D. Boneh and M. Franklin, Proceedings CRYPTO '99, LNCS, Vol. 1666, Springer-Verlag, pp. 1-13, i-iv, 1999.
	PUBLICATION: "Collusion-Secure Fingerprinting for Digital Data". D. Boneh and J. Shaw. IEEE Transactions on Information Theory, Vol. 44, No. 5, pp. 1897-1905, 1998.
↓	PATENT APPLICATION: "Forensic Media Key Block for Identifying Compromised Keys". Lotspiech. Co-pending application serial no. 09/564,658, filed May 3, 2000.
	PUBLICATION: "Threshold Traitor Tracing". M. Naor and B. Pinkas, CRYPTO '98, LNCS vol. 1462, pp. 502-517, 1998.



PUBLICATION: "Efficient Dynamic Traitor Tracing". O. Berkman, M. Parnas and J. Sgall. Proceedings of the 11th ACM-SIAM Symp. On Discrete Algorithms (SODA), PP. 586-595, 2000.

PUBLICATION: "Tracing Traitors". B. Chor, A. Fiat, M. Naor and B. Pinkas. IEEE Transactions on Information Theory, Vol. 46, No. 3, May 2000.

REPORT: "Key Management for Multicast: Issues and Architectures". D. Waller, E. Harder, and R. Agee. National Security Agency, pp. 1-19, June 1999.

PUBLICATION: "On the Generation of Cryptographically Strong Pseudorandom Sequences". Adi Shamir, ACM Transactions on Computer Systems, vol. 1, no. 1, pp. 38-44, February 1983.

Examiner

Date Considered

5/9/05

Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).